POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO DO GRUPO BGS

Versão 1.0

- BRASIMPEX Distribuidora de Equipamentos de Segurança e Esportivos LTDA
- GRIMP Equipamentos de Segurança LTDA
- BGS América LTDA

Brasília – DF
21 de maio de 2026

SUMÁRIO

1. APRESENTAÇÃO

1.1 A presente Política de Confidencialidade e Segurança da Informação (PCSI) estabelece os princípios, diretrizes, responsabilidades e controles gerais relacionados à proteção das informações, dados pessoais, ativos tecnológicos, sistemas e documentos tratados pelo Grupo BGS.

1.2 Esta Política integra o Programa de Integridade e Compliance do Grupo BGS e tem como finalidade promover a proteção adequada das informações institucionais, estratégicas, comerciais, técnicas, operacionais e pessoais tratadas pela organização, assegurando a continuidade das atividades empresariais, a mitigação de riscos operacionais, reputacionais e jurídicos, bem como a conformidade com a legislação aplicável.

1.3 Aplica-se às empresas integrantes do Grupo BGS e demais empresas e unidades vinculadas ao Grupo.

2. REFERÊNCIAS NORMATIVAS E LEGAIS

2.1 Esta Política observa a seguinte legislação:

- 2.1.1 Lei nº 14.133/2021 (Lei de Licitações);
- 2.1.2 Lei nº 13.709/2018 (LGPD);
- 2.1.3 Lei nº 12.965/2014 (Marco Civil da Internet);
- 2.1.4 Lei nº 12.846/2013 (Lei Anticorrupção);
- 2.1.5 Lei nº 8.078/1990 (Código de Defesa do Consumidor)
- 2.1.6 Decreto-Lei nº 5.452/1943 (CLT);
- 2.1.7 Decreto-Lei nº 2.848/1940 (Código Penal).

2.2 Adicionalmente, o Grupo BGS adota como referência de boas práticas:

- 2.2.1 ISO/IEC 27001;
- 2.2.2 ISO/IEC 27002;
- 2.2.3 ISO/IEC 27701;
- 2.2.4 princípios de governança corporativa e gestão de riscos aplicáveis à segurança da informação.

3. OBJETIVO

3.1 Estabelecer diretrizes, princípios e controles voltados à proteção das informações institucionais, à prevenção de acessos não autorizados, à preservação da confidencialidade, integridade, disponibilidade e rastreabilidade das informações, à mitigação de riscos relacionados à segurança da informação e proteção de dados, bem como à conscientização de colaboradores, parceiros e terceiros quanto às boas práticas de segurança da informação e confidencialidade adotadas pelo Grupo BGS.

4. ABRANGÊNCIA

4.1 Esta Política aplica-se a:

- 4.1.1 administradores e sócios
- 4.1.2 diretores e gestores
- 4.1.3 colaboradores
- 4.1.4 prestadores de serviços
- 4.1.5 representantes comerciais
- 4.1.6 fornecedores e parceiros
- 4.1.7 terceiros que tenham acesso a informações do Grupo BGS.

4.2 A Política abrange informações armazenadas em meio físico, meio digital, ambientes em nuvem, dispositivos móveis, sistemas internos, redes corporativas, e ambientes remotos de trabalho.

5. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

5.1 O Grupo BGS adotará medidas voltadas à proteção das informações com base nos seguintes princípios:

- 5.1.1 **Confidencialidade**: Garantia de que as informações sejam acessadas apenas por pessoas autorizadas.
- 5.1.2 **Integridade**: Garantia de que as informações permaneçam completas, corretas e protegidas contra alterações indevidas.
- 5.1.3 **Disponibilidade**: Garantia de acesso às informações sempre que necessário às atividades autorizadas.

6. CLASSIFICAÇÃO DAS INFORMAÇÕES

6.1 As informações poderão ser classificadas conforme seu nível de sensibilidade:

6.1.1 **Pública**: Informações que podem ser livremente divulgadas interna e externamente sem causar impactos ao Grupo BGS, parceiros, clientes ou terceiros.

6.1.2 **De Uso Interno**: Informações destinadas às atividades internas da organização, cujo compartilhamento externo indevido não gera impactos críticos, mas deve ser evitado.

6.1.3 **Restrita**: Informações acessíveis apenas a departamentos, equipes ou pessoas especificamente autorizadas, cujo vazamento pode gerar impactos operacionais, comerciais, estratégicos ou reputacionais ao Grupo BGS.

6.1.4 **Confidencial**: Informações altamente sensíveis, estratégicas, financeiras, tecnológicas ou protegidas por obrigação legal, contratual ou regulatória, cujo acesso deve ser estritamente controlado e cujo vazamento pode causar danos relevantes financeiros, jurídicos, operacionais ou reputacionais ao Grupo BGS ou a terceiros.

7. GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

7.1 A governança da segurança da informação será conduzida pelo Comitê de Gestão da Segurança da Informação (CGSI), responsável por:

7.1.1 supervisionar as diretrizes de segurança;

7.1.2 acompanhar riscos e incidentes;

7.1.3 propor melhorias;

7.1.4 apoiar a implementação de controles;

7.1.5 promover cultura organizacional de segurança.

7.2 A estrutura de governança poderá incluir:

7.2.1 Responsável pelo Programa de Segurança da Informação;

7.2.2 Encarregado pelo Tratamento de Dados Pessoais (DPO);

7.2.3 representantes técnicos e administrativos.

7.3 As atribuições específicas poderão ser detalhadas em normas internas complementares.

8. CONTROLE DE ACESSO

8.1 O acesso às informações, sistemas e ativos tecnológicos do Grupo BGS deverá observar os seguintes princípios e controles:

- 8.1.1 princípio do menor privilégio;
- 8.1.2 necessidade funcional;
- 8.1.3 segregação de funções;
- 8.1.4 controle individualizado de usuários;
- 8.1.5 rastreabilidade de acessos;
- 8.1.6 revisão periódica de permissões;
- 8.1.7 revogação imediata de acessos em caso de desligamento, alteração de função ou perda de autorização.

8.2 O compartilhamento de credenciais é expressamente proibido.

9. SENHAS E CREDENCIAIS

9.1 As credenciais de acesso aos sistemas, redes e ativos tecnológicos do Grupo BGS deverão observar padrões mínimos de segurança definidos pela organização.

9.2 As senhas deverão ser individuais, confidenciais e protegidas contra acesso não autorizado, sendo expressamente proibido seu compartilhamento.

9.3 Sempre que tecnicamente viável, deverão ser adotados mecanismos adicionais de proteção, incluindo autenticação multifator (MFA), especialmente em sistemas críticos, administrativos ou que tratem informações sensíveis.

9.4 Qualquer suspeita de comprometimento de credenciais deverá ser comunicada imediatamente aos responsáveis designados pelo Grupo BGS.

10. USO DE EQUIPAMENTOS E SISTEMAS

10.1 Os equipamentos e sistemas disponibilizados pelo Grupo BGS destinam-se prioritariamente às atividades profissionais.

10.2 É vedado: instalar softwares não autorizados; compartilhar arquivos institucionais sem autorização; armazenar informações institucionais em locais inseguros; utilizar sistemas corporativos para atividades ilícitas ou incompatíveis com os interesses do Grupo BGS.

10.3 Os ativos tecnológicos corporativos pertencem ao Grupo BGS e poderão ser monitorados, auditados e rastreados, observados os limites legais aplicáveis e os direitos fundamentais dos usuários.

11. PROTEÇÃO DE DADOS E CONFIDENCIALIDADE

11.1 Todos os colaboradores e terceiros deverão preservar o sigilo das informações às quais tiverem acesso.

11.2 Informações estratégicas, comerciais, técnicas, financeiras ou relacionadas a clientes e órgãos públicos não poderão ser divulgadas sem autorização formal.

11.3 A obrigação de confidencialidade permanece válida mesmo após o encerramento do vínculo contratual ou profissional.

12. BACKUP E PRESERVAÇÃO DAS INFORMAÇÕES

12.1 O Grupo BGS poderá adotar mecanismos de backup periódico e proteção contra perda de dados.

12.2 Os responsáveis pelos sistemas deverão observar medidas razoáveis para preservação da continuidade operacional.

13. GESTÂO DE INCIDENTES DE SEGURANÇA

13.1 Qualquer suspeita de: vazamento de informações; acesso indevido; perda de dados; comprometimento de sistemas; tentativa de fraude e incidente cibernético deverá ser comunicada imediatamente aos responsáveis designados pelo Grupo BGS.

13.2 Os incidentes poderão ser investigados e tratados conforme sua criticidade e impacto institucional. O Grupo BGS poderá manter procedimentos específicos para resposta a incidentes de segurança.

14. RELAÇÃO COM TERCEIROS

14.1 O Grupo BGS poderá exigir de terceiros:

14.1.1 compromissos formais de confidencialidade;

14.1.2 adoção de medidas mínimas de segurança da informação;

14.1.3 cumprimento da legislação aplicável relacionada à proteção de dados e segurança.

15. TREINAMENTO E CONSCIENTIZAÇÃO

15.1 O Grupo BGS promoverá ações periódicas de conscientização e treinamento relacionadas à proteção de informações; boas práticas de segurança; prevenção de fraudes; prevenção de engenharia social e proteção de dados pessoais.

16. DOCUMENTOS COMPLEMENTARES

16.1 Esta Política poderá ser complementada por:

16.1.1 normas internas;

16.1.2 procedimentos operacionais;

16.1.3 matriz de riscos específicos;

16.1.4 manuais técnicos;

16.1.5 planos de continuidade de atividade;

16.1.6 procedimentos de resposta a incidentes;

16.1.7 diretrizes de controle de acesso;

16.1.8 normas de backup e retenção documental.

17. DISPOSIÇÕES FINAIS

17.1 O Grupo BGS poderá implementar mecanismos de monitoramento de acessos, sistemas e ativos tecnológicos, observados os limites legais aplicáveis.

17.2 O descumprimento desta Política poderá resultar na adoção de medidas administrativas, disciplinares, contratuais e legais cabíveis.

17.3 A presente Política deverá ser divulgada internamente e observada por todos os integrantes e terceiros relacionados ao Grupo BGS.

17.4 Esta Política deverá ser revisada sempre que houver:

17.4.1 alterações legais;

17.4.2 mudanças organizacionais relevantes;

17.4.3 evolução tecnológica;

17.4.4 novos riscos relevantes;

17.4.5 incidentes significativos de segurança.

18. COMPROMISSO DA ALTA ADMINISTRAÇÃO

18.1 A Alta Administração do Grupo BGS reafirma seu compromisso com a proteção das informações institucionais, a segurança dos ativos tecnológicos e a confidencialidade dos dados tratados pela organização, apoiando integralmente a aplicação desta Política e a adoção contínua de boas práticas de segurança da informação.

JEAN PIERRE PAUL SUBLON:65919424168

Assinado de forma digital por JEAN PIERRE PAUL SUBLON:65919424168
Dados: 2026.05.21 12:06:14 -03'00'

Jean Pierre Paul Sublon

Presidente do Grupo BGS

A. CONTROLE DE VERSÕES

Versão	Data	Link para verificação de Integridade do documento
1.0	21/05/2026	https://docs.google.com/spreadsheets/d/12VI8K3Nmjflyf3HnkZAZTV-eDeyjfPUQqxsJj9HhPI8/edit?usp=sharing